In the Claims:

Please cancel claims 20-21, 23-24, 26-27, and 29-30. Please amend claims 5-7, 10-12, and 31-32. The claims are as follows:

1-4. (Canceled)

5. (Previously presented) A method of operating an intrusion detection system, comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service intrusion attempting to impede operation of the protected device~~; and~~,

wherein the intrusion detection system comprises an intrusion detection server and an intrusion detection sensor,

wherein the intrusion detection sensor is coupled to the intrusion detection server and to the protected device,

wherein the intrusion detection sensor comprises a governor, a programmable processor that oversees operation of the intrusion detection sensor, and a signature file,

wherein the governor includes a log, a timer, an alert generation rate threshold, and one or more rules that prescribe actions to be taken in order to decrease the generation rate of alerts by the intrusion detection sensor when the present alert generation rate exceeds the alert generation rate threshold,

wherein operation of the timer, utilization of the alert generation rate threshold, and implementation of the one or more rules are carried out by instructions executed by the programmable processor,

wherein the log consists of a list of timestamps that record the times at which the intrusion detection sensor generates alerts,

wherein the signature file includes a signature set comprising elements that include a signature set identifier, a signature event, a signature event counter that keeps count of the number of occurrences of the signature event, a signature threshold quantity, and a signature threshold interval, and

wherein the signature event includes a bit pattern that identifies the signature event;

~~when a~~ responsive to said monitoring determining that the signature event occurs, increasing a value of [[a]] the signature event counter and comparing the value of the signature event counter with [[a]] the signature threshold quantity; ~~and~~

adjusting the value of the signature event counter to not include a count of signature events past a sliding window specified by the signature threshold interval; and

for each occurrence of the value of the signature event counter exceeding the signature threshold quantity:

generating an alert by [[an]] the intrusion detection sensor ~~of the intrusion detection system,~~;

after said generating, recording in the log a timestamp denoting a time of generating the alert, said time of generating the alert derived from the timer ~~in a log of a governor comprised by the intrusion detection sensor,~~;

after said recording, clearing the log of any entries that are past a permissible age, said permissible age equal to a ratio of a cap imposed by the governor upon a rate of generation of alerts by the intrusion detector sensor to the alert generation rate threshold;

after said clearing, determining from contents of the log [[a]] the present alert generation rate, said determining the present alert generation rate comprising dividing the number of timestamps in the log by the permissible age; ~~and~~

after said determining, comparing the present alert generation rate with [[an]] the alert generation rate threshold, said comparing ascertaining that the present alert generation rate exceeds the alert generation rate threshold ~~recording is performed after said generating is performed, wherein said determining is performed after said recording is performed, and wherein said comparing the present alert generation rate with the alert generation rate threshold is performed after said determining is performed; and~~

~~for each occurrence of the present alert generation rate exceeding the alert generation rate threshold,~~;

responsive to said ascertaining that the present alert generation rate exceeds the alert generation rate threshold, altering an element of [[a]] the signature set ~~of the intrusion detection system~~ to decrease ~~an alert generation~~ a rate at which alerts are generated by [[of]] the intrusion detection sensor, said altering the element being implemented in accordance with said one or more rules.

6. (Currently amended) The method of claim 5, wherein the element is the signature threshold quantity, and wherein said altering the element comprises increasing the signature threshold quantity.

7. (Currently amended) The method of claim 5, wherein the element is [[a]] the signature threshold interval that specifies a sliding time window, and wherein said altering the element comprises decreasing the signature threshold interval.

8-9. (Canceled)

10. (Currently amended) Programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service intrusion attempting to impede operation of the protected device~~; and~~,

wherein the intrusion detection system comprises an intrusion detection server and an intrusion detection sensor,

wherein the intrusion detection sensor is coupled to the intrusion detection server and to the protected device,

wherein the intrusion detection sensor comprises a governor, a programmable processor that oversees operation of the intrusion detection sensor, and a signature file,

wherein the governor includes a log, a timer, an alert generation rate threshold, and one or more rules that prescribe actions to be taken in order to decrease the generation rate of alerts by the intrusion detection sensor when the present alert generation rate exceeds the alert generation rate threshold,

wherein operation of the timer, utilization of the alert generation rate threshold, and implementation of the one or more rules are carried out by instructions executed by the programmable processor,

wherein the log consists of a list of timestamps that record the times at which the intrusion detection sensor generates alerts,

wherein the signature file includes a signature set comprising elements that include a signature set identifier, a signature event, a signature event counter that keeps count of the number of occurrences of the signature event, a signature threshold quantity, and a signature threshold interval, and

wherein the signature event includes a bit pattern that identifies the signature event;

~~when a~~ responsive to said monitoring determining that the signature event occurs, increasing a value of [[a]] the signature event counter and comparing the value of the signature event counter with [[a]] the signature threshold quantity; ~~and~~

adjusting the value of the signature event counter to not include a count of signature events past a sliding window specified by the signature threshold interval; and

for each occurrence of the value of the signature event counter exceeding the signature threshold quantity:

generating an alert by [[an]] the intrusion detection sensor ~~of the intrusion detection system,~~;

after said generating, recording in the log a timestamp denoting a time of generating the alert, said time of generating the alert derived from the timer ~~in a log of a governor comprised by the intrusion detection sensor,~~;

after said recording, clearing the log of any entries that are past a permissible age, said permissible age equal to a ratio of a cap imposed by the governor upon a rate of generation of alerts by the intrusion detector sensor to the alert generation rate threshold;

after said clearing, determining from contents of the log [[a]] the present alert generation rate, said determining the present alert generation rate comprising dividing the number of timestamps in the log by the permissible age; ~~and~~

after said determining, comparing the present alert generation rate with [[an]] the alert generation rate threshold, said comparing ascertaining that the present alert generation rate exceeds the alert generation rate threshold ~~recording is performed after said generating is performed, wherein said determining is performed after said recording is performed, and wherein said comparing the present alert generation rate with the alert generation rate threshold is performed after said determining is performed; and~~

~~for each occurrence of the present alert generation rate exceeding the alert generation rate threshold,~~;

responsive to said ascertaining that the present alert generation rate exceeds the alert generation rate threshold, altering an element of [[a]] the signature set ~~of the intrusion detection system~~ to decrease ~~an alert generation~~ a rate at which alerts are

generated by [[of]] the intrusion detection ~~server~~ sensor, said altering the element being implemented in accordance with said one or more rules.

11. (Currently amended) The programmable media of claim 10, wherein the element is the signature threshold quantity, and wherein said altering the element comprises increasing the signature threshold quantity.

12. (Currently amended) The programmable media of claim 10, wherein the element is [[a]] the signature threshold interval that specifies a sliding time window, and wherein said altering the element comprises decreasing the signature threshold interval.

13-18. (Canceled)

19. (Previously presented) The method of claim 5, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protected device.

20-21. (Canceled)

22. (Previously presented) The method of claim 5, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

23-24. (Canceled)

25. (Previously presented) The programmable media of claim 10, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protected device.

26-27. (Canceled)

28. (Previously presented) The programmable media of claim 10, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

29-30. (Canceled)

31. (Currently amended) The method of claim 5, further comprising the steps of:

awaiting, by the governor, for occurrence of a scheduled update time;

for each scheduled update time occurrence: clearing the log of any entries that are past ~~a specified~~ the permissible age, determining from contents of the log the current alert generation rate by dividing the number of timestamps in the log by the permissible age, and comparing the current alert generation rate with the alert generation rate threshold; and

for each occurrence of the current alert generation rate exceeding the alert generation rate threshold: ascertaining that [[a]] the signature set of the intrusion detection system is at its initial state at which no changes in the signature set have been made by the governor, and altering one or more elements of the signature set in response to said ascertaining.

32. (Currently amended) The programmable media of claim 10, wherein the programmable software further comprises the steps of:

awaiting, by the governor, for occurrence of a scheduled update time;

for each scheduled update time occurrence: clearing the log of any entries that are past ~~a~~ ~~specified~~ the permissible age, determining from contents of the log the current alert generation rate by dividing the number of timestamps in the log by the permissible age, and comparing the current alert generation rate with the alert generation rate threshold; and

for each occurrence of the current alert generation rate exceeding the alert generation rate threshold: ascertaining that [[a]] the signature set of the intrusion detection system is at its initial state at which no changes in the signature set have been made by the governor, and altering one or more elements of the signature set in response to said ascertaining.